PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04N 7/16, 7/173 — A1

(11) International Publication Number: **WO 00/67483**

(43) International Publication Date: 9 November 2000 (09.11.00)

(21) International Application Number: PCT/US00/09800

(22) International Filing Date: 12 April 2000 (12.04.00)

(30) Priority Data:
60/132,366 4 May 1999 (04.05.99) US

(71) Applicant *(for all designated States except US)*: GENERAL INSTRUMENT CORPORATION [US/US]; 101 Tournament Drive, Horsham, PA 19044 (US).

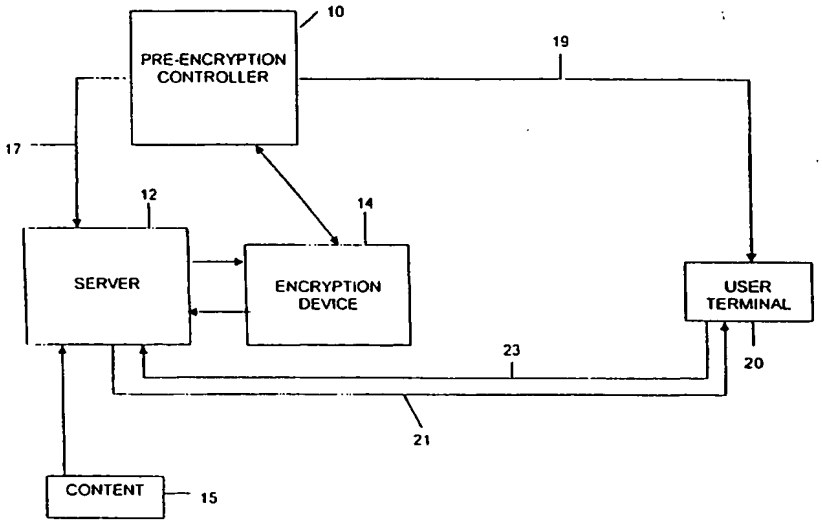
(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: SAFADI, Reem [US/US]; 429 Brown Briar Circle, Horsham, PA 19044 (US). VINCE, Lawrence, D. [US/US]; 114 Aileen Drive, Lansdale, PA 19446 (US).

(74) Agent: LIPSITZ, Barry, R.; 755 Main Street, Building No. 8, Monroe, CT 06468 (US).

(81) Designated States: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: METHOD AND APPARATUS FOR ACCESS CONTROL OF PRE-ENCRYPTED ON-DEMAND TELEVISION SERVICES



(57) Abstract

A method and apparatus for providing access control of pre-encrypted on-demand television content. Existing encryption capability for cable television services or the like is extended to handle pre-encrypted content from a server (12) that is requested on demand by a viewer at a user terminal (20). Alternatively, the pre-encrypted content (provided, e.g. by an encryption device (14) can be broadcast or multicast from the server (12) to a group of viewers. The invention is upgradeable to facilitate implementations of entitlement control algorithms that vary in sophistication as the need dictates. Additionally, the method is extensible to enable access control of pre-encrypted content that is independent of the transport protocol used. Such protocols include, for example, MPEG-2 and Internet Protocol (IP) which may also utilize Public Key Cryptography.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

METHOD AND APPARATUS FOR ACCESS CONTROL OF PRE-ENCRYPTED ON-DEMAND TELEVISION SERVICES

This application claims the benefit of U.S. provisional patent application no.60/132,366 filed May 4, 1999.

BACKGROUND OF THE INVENTION

The present invention relates to the communication of information services over a communication network, and more particularly to providing access control for signals containing audiovisual content and services, such as on-demand television programming. In order to render subscription programming services and the like commercially viable, systems must be provided for preventing non-paying individuals from obtaining the services. Such "access control" systems can take various forms, but generally include some type of modification (e.g., scrambling) or encryption of the signals that carry the services. Only authorized subscribers have access to the elements (e.g., cryptographic keys) necessary to satisfactorily receive the signals.

Current techniques for decryption of signals such as on-demand services may be based on real time hardware based encryption solutions or based on pre-encryption methods. Some configurations allow for

cost effective real time encryption at the transport level but are not as effective at a service level. Such problems, together with the following additional factors, require a new solution that provides a reliable and cost-effective means for access control of on-demand services:

1. Current real-time encryption does not meet the cost model for on-demand services, in that it is expensive to implement.
2. In some configurations real time encryption requires too much real-estate at service provider sites (currently, for example, various video-on-demand (VOD) vendors are consolidating their servers and signal modulators (e.g., QAM modulators) in space efficient packaging which bypasses a real-time encryption stage).
3. Pre-encryption is inherently not as secure as real-time encryption. At the same time, on-demand content security requirements are less stringent than those of broadcast content. For example, there is no *a priori* knowledge of when certain content will be requested in the on-demand case. In the broadcast case, the content is always being sent and the schedules are known ahead of time.
4. MPAA (Motion Picture Association of America) has issues with clear (i.e., unencrypted)

content, such as movies, and expects such content to be protected.

5. Entitlement control should be upgradeable without impacting content providers or server vendors. Stronger solutions should be able to be incorporated gradually as the need dictates.

6. Secure content delivery of MPEG-2 (Motion Picture Experts Group) using Internet Protocol (IP) for point to point on demand services or multicast services must be facilitated.

7. Transport independent entitlement control (e.g., MPEG-2 or IP) must be provided.

It would be advantageous to provide a method and apparatus for access control of on-demand services that addresses the above-noted issues. In particular, it would be advantageous to provide a content pre-encryption method that enables entitlement control to be effectively implemented independent of the transport protocol, e.g., MPEG-2 or IP.

It would be still further advantageous to provide such a capability that can be offered as a separate service to content providers, server vendors, and cable system operators. The present invention can be adapted for use with different

types of provider networks, e.g. satellite and Internet based networks.

The present invention provides a system having these and other advantages. In particular, the invention disclosed herein extends existing encryption capability, such as that provided by the Digicipher II (DCII) system available from General Instrument Corporation of Horsham, Pennsylvania, USA, the assignee of the present invention, to handle pre-encrypted content that is requested on demand by a viewer or is sent to a group of viewers. The method of the invention is also upgradeable to facilitate implementations of entitlement control algorithms that vary in sophistication as the need dictates. Additionally, the method is extensible to enable encryption control that is independent of the transport protocol used. Such protocols include, for example, MPEG-2 and Internet Protocol (IP).

SUMMARY OF THE INVENTION

In accordance with the present invention, a method and apparatus are provided for access control of pre-encrypted on-demand content. In a simplified embodiment, the content is pre-encrypted by an encryption device controlled by a pre-encryption controller. The pre-encrypted content is forwarded from the encryption device to a server. The server may be a main server or a local distribution server. The pre-encryption controller provides a first tag to the user terminal and a second tag to the server. Said first tag being associated with said second tag and said second tag acts as a reference to the pre-encrypted content and associated first tag, wherein said first and second tags are unique to the pre-encrypted content and are tracked by the pre-encryption controller. The pre-encrypted content is communicated from the server to a user terminal via a first communication path.

An entitlement authorization associated with the encrypted content is communicated to a user terminal (e.g., a "client device" such as a set-top box) via a second communication path independent of said first communication path. Authorization to access the pre-encrypted content is determined based on said entitlement authorization and said first tag upon demand of said content by a user.

The user terminal may be a set-top box, a

digital television or a host with point-of-deployment (POD) capability, or a personal computer (PC) or the like that provides the functionality of a set-top box.

The pre-encryption controller acts to set up the encryption device for pre-encrypting the content. The set up of the encryption device is outside the scope of this invention. For background purposes, it will suffice to state that the pre-encryption controller, through bi-directional communication with the encryption device, configures the encryption device with appropriate parametric values and commands to enable the encryption device appropriately to encrypt the content.

In an alternate embodiment, the server is a main server (e.g., a head-end server) which communicates the pre-encrypted content and first tag to the user terminal via a local distribution server. The pre-encryption controller is in communication with a local distribution controller (e.g., a head-end controller in a cable television implementation), which local distribution controller communicates the entitlement authorization to the user terminal.

In a preferred embodiment, the first tag is an opaque data block (ODB) and the second tag is a unique reference handle (URH). The URH may be generated as a function of the ODB.

In one embodiment, the ODB and URH are both

forwarded to both the local distribution controller and the server from the pre-encryption controller. In an alternate embodiment, only the URH is forwarded to the main server and the ODB is communicated from the local distribution controller to the local distribution server.

In one embodiment the ODB or the URH may be stored as an attribute of the encrypted content. Alternatively, both the URH and the ODB are stored as an attribute of the encrypted content.

The ODB may be processed at the local distribution controller to generate a second ODB, which second ODB is forwarded from the local distribution controller to the local distribution server. This processing at the local distribution controller may include algorithmically modifying the ODB. Such reprocessing of the ODB at the local distribution controller provides an added level of security since the post-processing ODBs are no longer the same across multiple local distribution controllers.

The ODB itself may be coded in a manner that is not readily discernable by third parties. Alternatively, the ODB content may include an encryption key to be used for decryption or used to derive the key for decryption. The ODB may also include a hierarchy of encryption keys whose ultimate use is the derivation of the relevant key for decryption but with added levels of security. In

this manner the ODB content is securable as deemed necessary without burdening the content providers or service vendors. In the on-demand case, the ODB itself may also be encrypted, using, for example, the recipient's public key.

The pre-encrypted content may be broadcast, multicast, or singlecast such that only a user terminal with appropriate entitlement authorization will be able to decrypt the broadcast, multicast, or singlecast content. Alternatively, the pre-encrypted content may be accessed via the Internet.

The entitlement authorization may comprise at least one of (i) an entitlement authorization for a service carrying the content, (ii) an entitlement authorization for the content itself, and (iii) an entitlement authorization for using ODB.

In a preferred embodiment, a client application (typically software residing in a user terminal such as a set-top box) then requests specific content from the server, such as a video on demand (VOD) movie or any other interactive content. The ODB is forwarded from a server application to the client application software that typically resides in a central processor (CPU) of the user terminal. After this set-up is completed, the server starts sending the pre-encrypted content to the user terminal. The ODB is then forwarded from the client application via an application program interface in the CPU to a kernel located in the user terminal. The ODB is then

processed in the user terminal in conjunction with the received entitlement authorization to determine whether to decrypt the received pre-encrypted content.

Processing may be provided by a secure processor located in the user terminal or a software task included in the user terminal CPU. The pre-encrypted content is received by the user terminal and decrypted when authorization is granted. Upon authorization, the content will be processed for display.

The pre-encrypted content may be received by the secure processor via a conventional receiver circuit. Alternatively, the pre-encrypted content may be received by the secure processor via direct memory access from device memory.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a block diagram of the functional components of the flexible pre-encryption architecture of the invention;

Figure 2 is a block diagram of another embodiment of the functional components of the flexible pre-encryption architecture of the invention; and

Figure 3 is a block diagram of the relevant components of a user terminal in accordance with the invention.

DETAILED DESCRIPTION OF THE INVENTION

Figure 1 illustrates the main components of an on-demand content communication system in accordance with the present invention. In particular, a method and apparatus are provided for access control of pre-encrypted on-demand content. The video encoder and post encoding processors are not shown, since they are well known in the art. As will be appreciated by those skilled in the art, any type of post processing to be done on the content file/data stream is performed prior to encryption.

Referring to Figure 1, a pre-encryption controller 10 sets up an encryption device 14 for encryption of the content 15. A server 12 forwards the content file/stream to the encryption device 14 for encryption of the content prior to distribution ("pre-encryption"). The encryption device encrypts the content file and forwards the pre-encrypted content back to the main server 12.

The pre-encryption controller 10 acts to set up the encryption device 14 for pre-encrypting the content. The set up of the encryption device 14 is outside the scope of this invention. For background purposes, it will suffice to state that the pre-encryption controller 10, through bi-directional communication with the encryption device 14, configures the encryption device 14 with appropriate parametric values and commands to enable the

encryption device 14 appropriately to encrypt the content.

In one embodiment as shown in Figure 1, the pre-encrypted content is forwarded from the encryption device 14 to a server 12. The server may be a main server or a local distribution server. The pre-encryption controller provides a first tag and a second tag to the server 12 via line 17. The first tag is also provided to a user terminal 20 via line 19 or 21 depending upon the particular implementation, the first tag being associated with said second tag. The second tag acts as a reference to the pre-encrypted content and associated first tag, wherein the first and second tags are unique to the pre-encrypted content and are tracked by the pre-encryption controller 10. The pre-encrypted content is communicated from the server 12 to a user terminal 20 (e.g., a "client device" such as a set-top box) via a first communication path 21.

An entitlement authorization associated with the encrypted content is communicated to the user terminal 20 via a second communication path 19 independent of the first communication path. Authorization to access the pre-encrypted content is determined at the user terminal 20 based on said entitlement authorization and the first tag upon demand of the content by a user. Communication from the user terminal 20 back to the server 12 is provided on line 23.

The user terminal 20 may be a set-top box, a digital television or a host with point-of-deployment (POD) capability, or a personal computer (PC) or the like that provides the functionality of a set-top box.

In an alternate embodiment shown in Figure 2, the server is a main server 12' (e.g., a head-end server) which communicates the pre-encrypted content and first tag to the user terminal 20 via lines 25 and 27 and a local distribution server 18. The main server 12' can distribute the encrypted content to various local distribution servers (at various service provider locations, e.g., head-ends). The pre-encryption controller 10 is in communication with a local distribution controller 16, which controls, e.g., a cable television system or the like in a well known manner (e.g., a head-end controller in a cable television implementation). The local distribution controller 16 communicates the entitlement authorization to the user terminal 20 via line 29.

In a preferred embodiment, the first tag is an opaque data block (ODB) and the second tag is a unique reference handle (URH). The URH may be generated as a function of the ODB.

In one embodiment, the ODB and URH are both forwarded to both the local distribution controller 16 (via line 11) and the main server 12' (via line 13) from the pre-encryption controller 10. In an

alternate embodiment, only the URH is forwarded to the main server 12' and the ODB is communicated from the local distribution controller 16 to the local distribution server 18 via line 22.

Either the ODB or the URH may be stored as an attribute of the encrypted content. Alternatively, both the URH and the ODB may be stored as an attribute of the encrypted content.

The ODB may be processed at the local distribution controller 16 to generate a modified, second ODB, which second ODB is forwarded from the local distribution controller 16 to the local distribution server 18. This processing at the local distribution controller 16 may include algorithmically modifying the ODB. This may be done as an offline process. Such reprocessing of the ODB at the local distribution controller 16 provides an added level of security since the post-processing ODBs are no longer the same across multiple local distribution controllers.

The system manufacturer specifies the ODB content and, for security reasons, the ODB itself may be coded in a manner that is not readily discernable by third parties. Alternatively, the ODB content may include an encryption key to be used for decryption or used to derive the key for decryption. The ODB may also include a hierarchy of encryption keys whose ultimate use is the derivation of the relevant key for decryption but with added levels of

security. In the on-demand case, the ODB itself may also be encrypted (with an additional level of implementation complexity) using, for example, the recipient's public key. In the case of broadcast or multicast content, the ODB may be made available in advance since it is associated with the event or content to be viewed or received. Encryption of the ODB using the user's public key is extremely useful for the IP transport case where the system administrator has to the option to make known what events are available when, e.g. via an Electronic Programming Guide (EPG). In this manner the ODB content is securable as deemed necessary without burdening the content providers or service vendors. In addition, the entitlement control is upgradeable without impacting the content providers or service vendors.

The pre-encrypted content may be broadcast, multicast, or singlecast such that only a user terminal 20 with appropriate entitlement authorization will be able to decrypt the broadcast, multicast, or singlecast content. Alternatively, the pre-encrypted content may be accessed via the Internet.

The entitlement authorization may comprise at least one of (i) an entitlement authorization for a service carrying the content, (ii) an entitlement authorization for the content itself, and (iii) an entitlement authorization for using ODB.

Figure 3 depicts the processing that takes place at the user terminal 20. The client application 40 (typically residing in a user terminal 20 such as a set-top box) then requests specific content from the server (either the server 12 of Figure 1 or local distribution server 18 of Figure 2), such as a video on demand (VOD) movie or any other interactive content. The server then sends the ODB to the client application device 40. After this set-up is completed, the server 18 starts sending the pre-encrypted content to the user terminal 20.

The client application 40 (e.g. software) running in the user terminal processor (CPU) 36 receives the ODB from a server application in the server 12 or local distribution server 18, as described in connection with Figures 1 and 2, and forwards it via an application program interface (API) 42 to the user terminal processor kernel 44. In the broadcast and multicast modes, the ODB may be made available ahead of time, before the actual broadcast or multicast event commences. In this case the ODB may be requested by and sent to the user by the local distribution controller (16). The ODB is then processed in the user terminal 20 in conjunction with the received entitlement authorization (as described in connection with Figures 1 and 2) to determine whether to decrypt the received pre-encrypted content.

Processing may be provided by a secure processor 32 located in the user terminal 20 or a software task included in the CPU 36. The pre-encrypted content is received by the user terminal 20 and decrypted when authorization is granted. Upon authorization, the content will be processed for display.

The pre-encrypted content may be received by the secure processor 32 via a conventional receiver circuit (i.e. receiver output of Figure 3). Alternatively, the pre-encrypted content may be received by the secure processor 32 via direct memory access from device memory 30. The decrypted output from the secure processor 32 is written back to memory 30 for further use by the CPU 36, or is forwarded to a demultiplexer/decoder 34 for further processing in a conventional manner.

It should now be appreciated that the present invention provides an improved method and apparatus for the delivery and access of pre-encrypted on-demand television services. In particular, the present invention provides a content pre-encryption method and apparatus that enables entitlement control to be effectively implemented independent of the transport protocol, e.g., MPEG-2 or Internet Protocol (IP), and to some extent independent of transmission mode (i.e., singlecast (e.g., on-demand), multicast, or broadcast). Additionally, the present invention provides encryption and access

control capability that can be offered as a separate service to content providers, server vendors, cable system operators, and/or Internet service providers, or the like. The present invention enables entitlement authorization that can vary in sophistication as deemed necessary without burdening the content providers or service vendors. In addition, the entitlement control is upgradeable without impacting the content providers or service vendors.

Although the invention has been described in connection with certain preferred embodiments, it should be appreciated that numerous adaptations and modifications may be made thereto without departing from the scope of the invention as set forth in the claims.

What is claimed is:

1. A method of providing access control for pre-encrypted on-demand content, comprising the steps of:

pre-encrypting the content;

forwarding the pre-encrypted content to a server;

providing a first tag to a user terminal, said first tag being associated with a second tag;

said second tag acting as a reference to the pre-encrypted content and associated first tag, wherein said first and second tags are unique to the pre-encrypted content and are tracked by a pre-encryption controller;

providing at least said second tag to said server;

communicating the pre-encrypted content from said server to said user terminal via a first communication path;

communicating an entitlement authorization associated with the pre-encrypted content to said user terminal via a second communication path independent of said first communication path; and

determining whether said user terminal is authorized to access said pre-encrypted content based on said entitlement authorization and said first tag upon demand of said content by a user.

2. A method in accordance with claim 1, wherein;

the server is a main server;

the main server communicates the pre-encrypted content and first tag to the user terminal via a local distribution server; and

the pre-encryption controller is in communication with a local distribution controller, which local distribution controller communicates the entitlement authorization to the user terminal.

3. A method in accordance with claim 2, wherein:

the first tag is an opaque data block (ODB); and

the second tag is a unique reference handle (URH).

4. A method in accordance with claim 3, comprising the further step of forwarding the ODB and associated URH to the local distribution controller.

5. A method in accordance with claim 3, wherein only the URH is forwarded to the main server, further comprising the steps of:

communicating the ODB from the local distribution controller to the local distribution server.

6. A method in accordance with claim 5, wherein the ODB is processed at the local distribution controller to generate a second ODB, which second

ODB is forwarded from the local distribution controller to the local distribution server.

7. A method in accordance with claim 3, wherein;

the pre-encrypted content is broadcast;

the ODB is broadcast; and

only a user terminal with appropriate entitlement authorization will be able to decrypt the broadcast content.

8. A method in accordance with claim 3, wherein:

the pre-encrypted content is multicast;

the ODB is multicast; and

only a user terminal with appropriate entitlement authorization will be able to decrypt the multicast content.

9. A method in accordance with claim 3, wherein:

the pre-encrypted content is singlecast;

the ODB is singlecast; and

only a user terminal with appropriate entitlement authorization will be able to decrypt the singlecast content.

10. A method in accordance with claim 3, wherein the entitlement authorization comprises at least one of (i) an entitlement authorization for a service carrying the content, (ii) an entitlement authorization for the content itself, and (iii) an entitlement authorization for using ODB.

11. A method in accordance with claim 3, further comprising the steps of:

forwarding the ODB from a server application via an application program interface in the user terminal to a kernel located in the user terminal;

processing the ODB in conjunction with the received entitlement authorization such that the processor determines whether to decrypt the received pre-encrypted content;

receiving the pre-encrypted content;

decrypting the pre-encrypted content when authorization is granted; and

processing the decrypted content for display.

12. A method in accordance with claim 11, wherein the pre-encrypted content is received by the secure processor via a receiver circuit.

13. A method in accordance with claim 11, wherein the pre-encrypted content is received by the secure processor via direct memory access from device memory.

14. A method in accordance with claim 3, wherein the ODB is coded in a manner that is not readily discernable by third parties.

15. A method in accordance with claim 3, wherein the ODB content includes one of an encryption key or a hierarchy of encryption keys.

16. A method in accordance with claim 3, wherein the ODB itself is encrypted.

17. A method in accordance with claim 16,

wherein the ODB is encrypted using the user's public key.

18. A method in accordance with claim 3, wherein the user terminal is one of a set-top box, a digital television or a host with point-of-deployment capability, or a personal computer.

19. A method in accordance with claim 3, wherein one of the URH and the ODB is stored as an attribute of the pre-encrypted content.

20. A method in accordance with claim 3, wherein each of the URH and the ODB are stored as an attribute of the pre-encrypted content.

21. A method in accordance with claim 3, wherein the pre-encrypted content is accessed via the Internet.

22. An apparatus for providing access control for pre-encrypted on-demand content, comprising:

an encryption device for encrypting the content;

a server for receiving the pre-encrypted content from the encryption device;

a pre-encryption controller for generating a first tag and an associated second tag, said second tag acting as a reference to the pre-encrypted content and associated first tag, wherein said first tag and second tag are unique to the pre-encrypted content and are tracked by the pre-encryption controller;

a user terminal for receiving entitlement

authorization associated with the pre-encrypted content;

said first tag being communicated to a user terminal and said second tag being communicated to the server;

wherein the user terminal determines whether it is authorized to access said pre-encrypted content based on said entitlement authorization and said first tag upon demand of said content by a user.

23. An apparatus in accordance with claim 22, wherein;

the server is a main server;

the main server communicates the pre-encrypted content and first tag to the user terminal via a local distribution server; and

the pre-encryption controller is in communication with a local distribution controller, which local distribution controller communicates the entitlement authorization to the user terminal.

24. An apparatus in accordance with claim 23, wherein:

the first tag is an opaque data block (ODB); and

the second tag is a unique reference handle (URH).

25. An apparatus in accordance with claim 24, wherein the local distribution controller receives the ODB and associated URH from the pre-encryption controller.

26. An apparatus in accordance with claim 24, wherein:

the main server receives only the URH from the pre-encryption controller; and

the local distribution controller communicates the ODB to the local distribution server.

27. An apparatus in accordance with claim 26, wherein the ODB is processed at the local distribution controller to generate a second ODB, which second ODB is forwarded from the local distribution controller to the local distribution server.

28. An apparatus in accordance with claim 24, wherein;

the pre-encrypted content is broadcast;

the ODB is broadcast; and

only a user terminal with appropriate entitlement authorization will be able to decrypt the broadcast content.

29. An apparatus in accordance with claim 24, wherein:

the pre-encrypted content is multicast;

the ODB is multicast; and

only a user terminal with appropriate entitlement authorization will be able to decrypt the multicast content.

30. An apparatus in accordance with claim 24, wherein:

the pre-encrypted content is singlecast;

the ODB is singlecast; and

only a user terminal with appropriate entitlement authorization will be able to decrypt the singlecast content.

31. An apparatus in accordance with claim 24, wherein the entitlement authorization comprises at least one of (i) an entitlement authorization for a service carrying the content, (ii) an entitlement authorization for the content itself, and (iii) an entitlement authorization for using ODB.

32. An apparatus in accordance with claim 24, wherein the user terminal comprises:

a client application using a program interface for forwarding the ODB from the local distribution server to a kernel

said kernel receiving the ODB the application program interface and the entitlement authorization from the local distribution controller; and

a secure processor for receiving the ODB and entitlement authorization from the kernel and receiving the pre-encrypted content from the local distribution server, wherein the processor processes the ODB in conjunction with entitlement authorization such that the processor determines whether to decrypt the received pre-encrypted content.

33. An apparatus in accordance with claim 32, wherein the secure processor receives the pre-encrypted content via a receiver circuit.

34. An apparatus in accordance with claim 32, wherein the secure processor receives the pre-encrypted content via direct memory access from device memory.

35. An apparatus in accordance with claim 24, wherein the ODB is coded in a manner that is not readily discernable by third parties.

36. An apparatus in accordance with claim 24, wherein the ODB content includes one of an encryption key or a hierarchy of encryption keys.

37. An apparatus in accordance with claim 24, wherein the ODB itself is encrypted.

38. An apparatus in accordance with claim 37, wherein the ODB is encrypted using the user's public key.

39. An apparatus in accordance with claim 24, wherein the user terminal is one of a set-top box, a digital television or a host with point-of-deployment capability, or a personal computer.

40. An apparatus in accordance with claim 24, wherein one of the URH and the ODB is stored as an attribute of the pre-encrypted content.

41. An apparatus in accordance with claim 24, wherein each of the URH and the ODB are stored as an attribute of the pre-encrypted content.

42. An apparatus in accordance with claim 24, wherein the pre-encrypted content is accessed via the Internet.

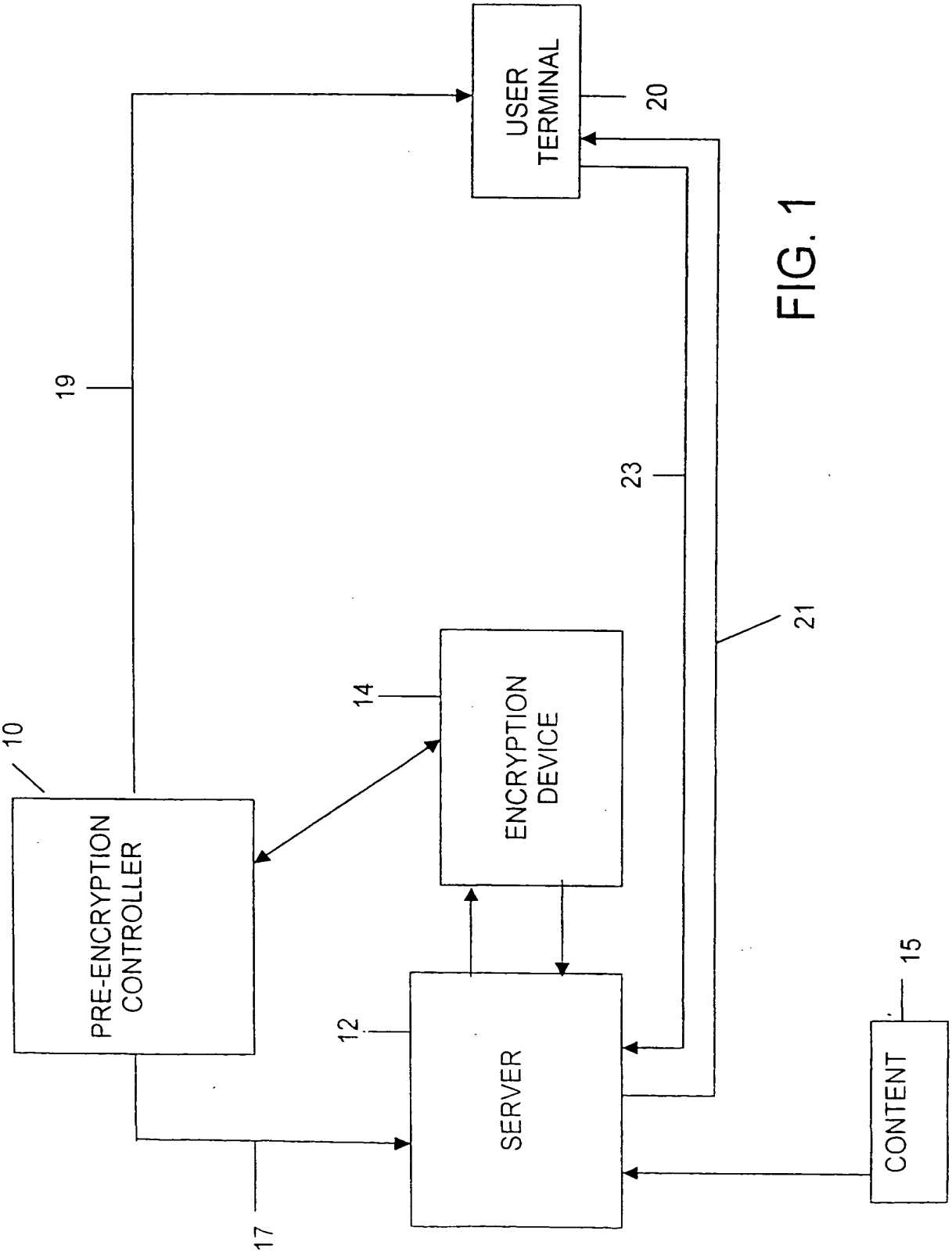


FIG. 1

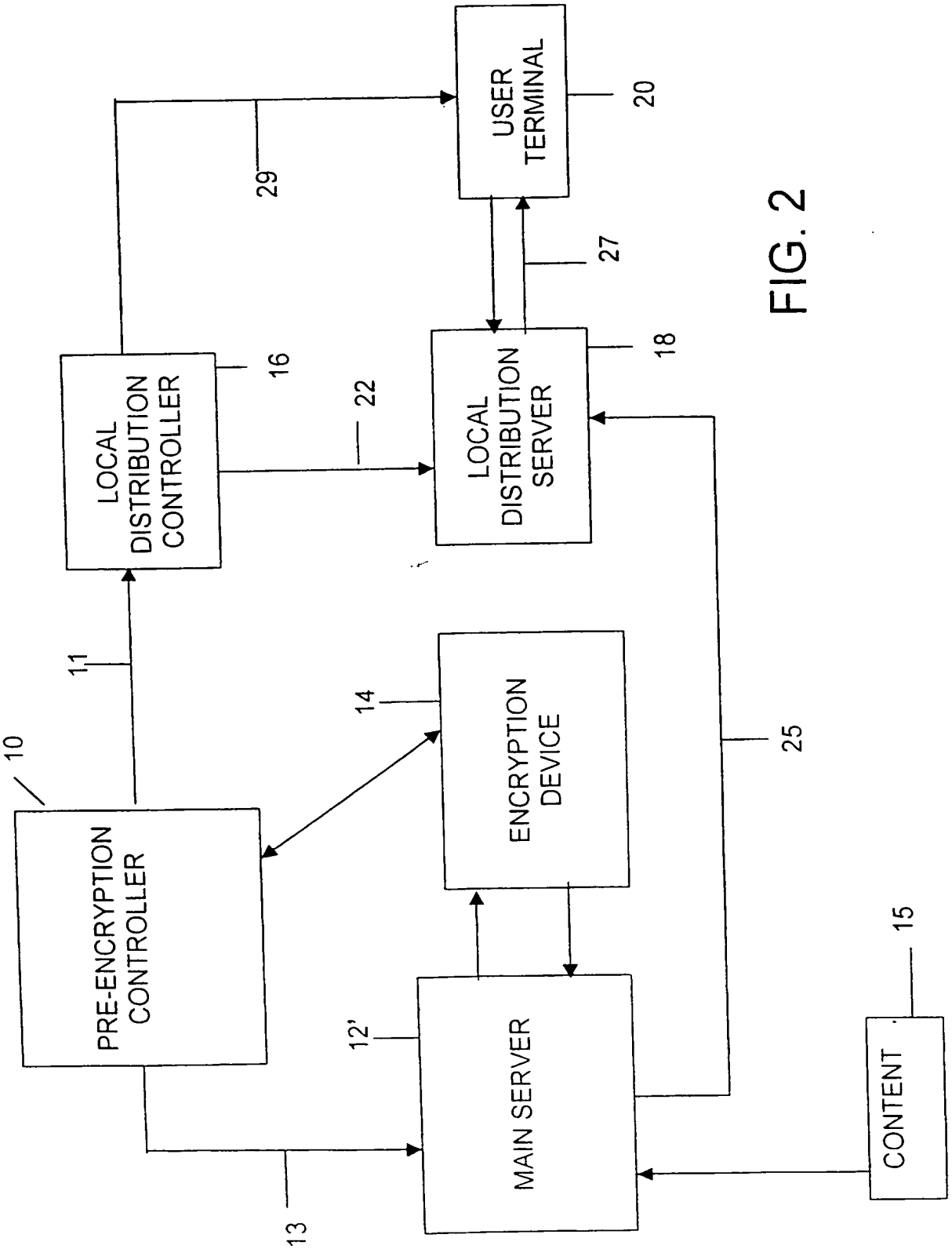

USER TERMINAL
20
29
27
LOCAL DISTRIBUTION CONTROLLER
16
22
LOCAL DISTRIBUTION SERVER
18
11
14
ENCRYPTION DEVICE
25
10
PRE-ENCRYPTION CONTROLLER
12'
MAIN SERVER
15
CONTENT
13

FIG. 2

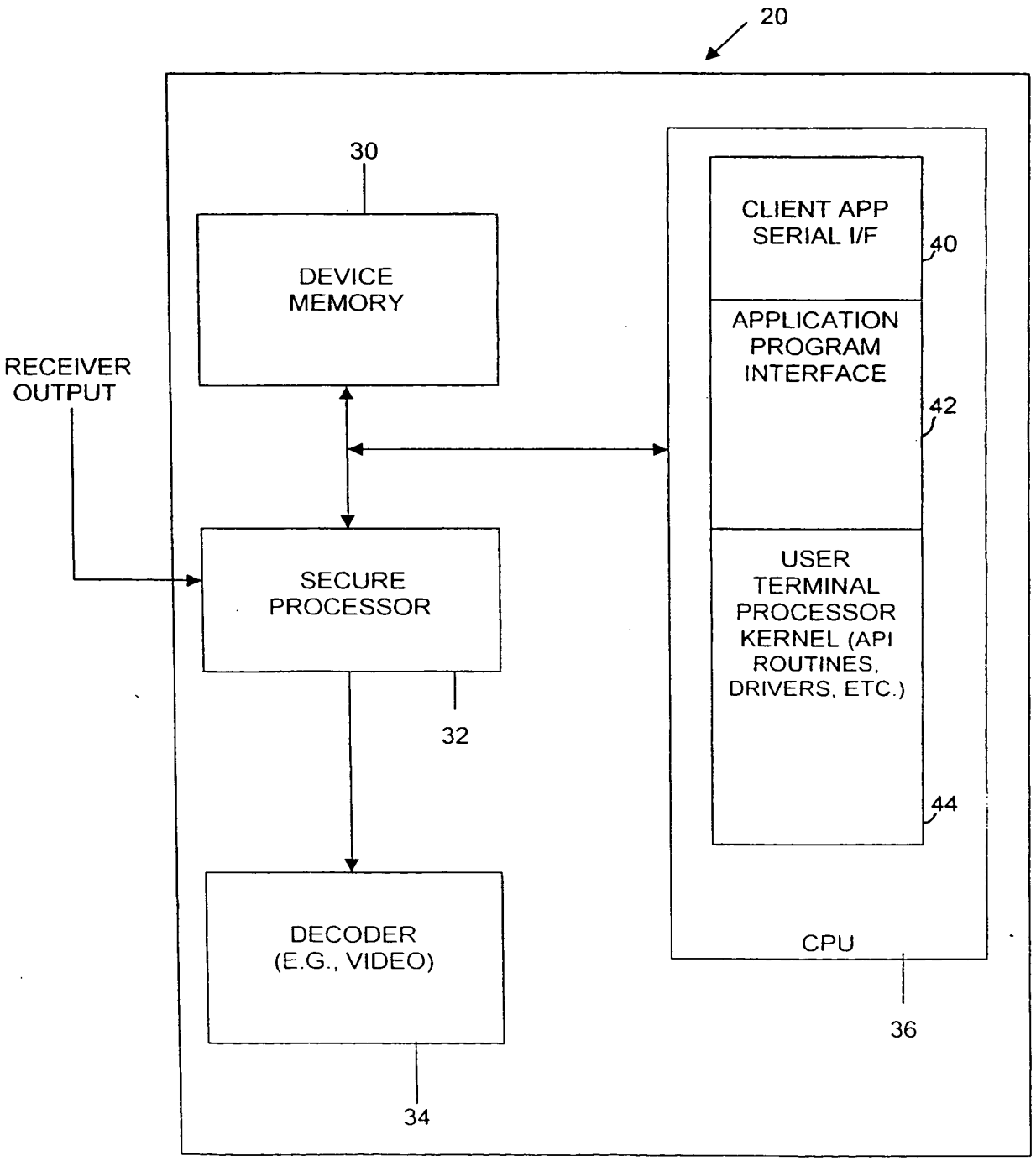


FIG. 3

INTERNATIONAL SEARCH REPORT

I. national Application No
PCT/US 00/09800

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04N7/16 H04N7/173

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 98 43426 A (TULLAYE PIERRE DE ;CANAL PLUS SA (FR); BAYASSI MULHAM (FR); JEZEQU) 1 October 1998 (1998-10-01) page 10, line 14 -page 16, line 19 page 19, line 18 -page 20, line 10	1-4, 7-18, 22-25, 28-39
A	EP 0 793 366 A (HITACHI LTD) 3 September 1997 (1997-09-03) page 3, column 3, line 55 -column 4, line 42 page 5, column 7, line 55 -column 8, line 50	1,2,22, 23
A	WO 99 14953 A (WORLDGATE COMMUNICATIONS INC) 25 March 1999 (1999-03-25) page 3, line 7 -page 4, line 4	21,42

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 July 2000	20/07/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Van der Zaal, R

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US 00/09800

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9843426 A	01-10-1998	AU 2770497 A	20-10-1998
		EP 0974229 A	26-01-2000
		NO 994532 A	19-11-1999
		PL 335585 A	08-05-2000
		AU 2770697 A	20-10-1998
		AU 7038198 A	20-10-1998
		WO 9843425 A	01-10-1998
		WO 9843162 A	01-10-1998
		WO 9843431 A	01-10-1998
		WO 9843248 A	01-10-1998
		WO 9843165 A	01-10-1998
		WO 9843415 A	01-10-1998
		WO 9843172 A	01-10-1998
		WO 9843433 A	01-10-1998
		WO 9843427 A	01-10-1998
		WO 9843437 A	01-10-1998
		WO 9843167 A	01-10-1998
		WO 9843428 A	01-10-1998
		WO 9843421 A	01-10-1998
		EP 0872798 A	21-10-1998
		EP 0866611 A	23-09-1998
		EP 0866616 A	23-09-1998
		EP 0866613 A	23-09-1998
		EP 0968610 A	05-01-2000
		EP 0968609 A	05-01-2000
		EP 0968607 A	05-01-2000
		EP 0974230 A	26-01-2000
		EP 0968468 A	05-01-2000
		EP 0968465 A	05-01-2000
		EP 0968602 A	05-01-2000
		EP 0968611 A	05-01-2000
		EP 0968608 A	05-01-2000
		EP 1010068 A	21-06-2000
		EP 1010331 A	21-06-2000
		EP 0968469 A	05-01-2000
		EP 1010320 A	21-06-2000
		EP 0972406 A	19-01-2000
		NO 994529 A	19-11-1999
		NO 994530 A	19-11-1999
		NO 994531 A	19-11-1999
		NO 994533 A	22-11-1999
		NO 994534 A	22-11-1999
		NO 994535 A	22-11-1999
		NO 994536 A	22-11-1999
		NO 994537 A	22-11-1999
		NO 994538 A	22-11-1999
		NO 994539 A	22-11-1999
		NO 994540 A	22-11-1999
		NO 994541 A	22-11-1999
EP 0793366 A	03-09-1997	JP 9230786 A	05-09-1997
		AU 693733 B	02-07-1998
		AU 1495297 A	18-09-1997
		AU 716807 B	09-03-2000
		AU 8786998 A	26-11-1998
		CN 1171682 A	28-01-1998
WO 9914953 A	25-03-1999	US 6049539 A	11-04-2000

INTERNATIONAL SEARCH REPORT

Information on patent family members

I. .national Application No
PCT/US 00/09800

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9914953 A		AU 9378398 A	05-04-1999
		NO 20001331 A	05-05-2000

Form PCT/ISA/210 (patent family annex) (July 1992)